



THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Southern District of New York](#)

Justice News

The New York State Department Of Financial Services Hearing On Law Enforcement And Virtual Currencies Prepared Testimony Of Deputy U.S. Attorney Richard B. Zabel

United States ~ Wednesday, January 29, 2014

Mr. Superintendent and distinguished members of the New York State Department of Financial Services: Thank you for the opportunity to appear before you today to discuss the law enforcement work of the United States Attorney's Office for the Southern District of New York and our federal agency partners in combating criminals and criminal enterprises that use virtual currencies to carry out their illegal activities. I am honored to represent the U.S. Attorney's Office at this hearing and to describe to you our approach to virtual currencies, some of our recent criminal cases in this emerging area, and some of the issues that we have observed and that concern us going forward.

The Government's Approach to the Criminal Use of Virtual Currencies

In our approach to virtual currencies, we recognize first of all that virtual currency systems can be legitimate, innovative global commerce mechanisms that may offer advantages over other forms of payment. Some advantages can be efficiency, cost benefits, and certain desired privacy features. Because we are not regulators, we do not focus on how to regulate and improve these emerging systems. Our concern is when the features of virtual currencies are exploited by criminals to carry out illegal conduct because the perpetrators feel they can more easily conceal their activity, their identities, and their proceeds. In attacking the criminal exploitation of virtual currencies, as in other areas of criminal law, we want to prosecute criminal conduct and maximize deterrence. To do so, we look to prosecute significant cases against individuals who are using or enabling others to use virtual currencies for criminal purposes and, where appropriate, we prosecute and shut down their illegal companies or websites as well.

Our approach therefore has been to look at the virtual currency criminal ecosystem and identify significant individuals and entities who enable that illegal ecosystem. In many ways, as with other traditional cases, we are following the money, but here it is the virtual money. Our attack on criminal virtual currency schemes accelerated when our office ramped up its focus on cybercrime

generally. At the beginning of his tenure in the summer of 2009, the U.S. Attorney, Preet Bharara, made combating cybercrime a priority of our office. We created the Complex Frauds Unit and we embedded in that Unit an expanded team of cyber prosecutors who focus almost exclusively on cybercrime, including virtual currencies. We have been fortunate that our great partners at Main Justice, the FBI, Secret Service, DEA, IRS, HSI, and other agencies have also made this effort a priority. And since many of these cases extend internationally, it has been important that we and our federal partners have developed relationships in the cybercrime area with prosecutors and law enforcement all around the world. That has been our approach and it has led to a number of significant prosecutions.

Recent Virtual Currency Criminal Cases

Let me briefly discuss three of our recent cases because they illustrate some of the problems we have identified at different levels of the criminal virtual currency ecosystem. All of these cases are pending so I will restrict myself to the public allegations as they are set forth in the charging documents and other public information. Of course all the defendants, unless they have pled guilty, are innocent until proven guilty. The first case is Liberty Reserve.

Liberty Reserve

As alleged, Liberty Reserve was in many ways the premier banking institution for cyber-criminals. It operated its own centralized digital currency commonly referred to as "LR." The company billed itself as the Internet's "largest payment processor and money transfer system," serving "millions" of people around the world, including the United States. It processed over 55 million illegal transactions and laundered more than \$6 billion in suspected proceeds of crimes including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking.

Liberty Reserve was deliberately designed and operated to enable criminal users to conduct financial transactions anonymously. Liberty Reserve was used extensively for illegal purposes, functioning as the bank of choice for the criminal underworld because it provided an infrastructure that enabled cyber criminals around the world to conduct anonymous and untraceable financial transactions. Liberty Reserve never registered with the U.S. Department of the Treasury as a money transmitting business, as it was required to do under U.S. law.

In order to use LR currency, a user first had to open an account through the Liberty Reserve website and provide basic identifying information; however, Liberty Reserve did not require users to validate their identities, and users routinely established accounts under false names. In fact, a federal agent in our investigation was able to set up an undercover account in the name "Joe Bogus" with an address of "123 Fake Main Street" in a city named "Completely Made Up City, New York." Once an account was established, the user could conduct transactions with other Liberty Reserve users. In these transactions, the user could receive transfers of LR from other users' accounts, and transfer LR from his or her own account to other users, including any "merchants" that accepted LR as payment. Liberty Reserve charged a fee for each transaction that was calculated as a percentage of the transaction value. And, for an additional "privacy fee," a user could hide his or her own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable.

Liberty Reserve did not permit users to fund their accounts by transferring money to the company directly through a credit card transfer or other means. Users also could not withdraw funds from their accounts directly. Instead, Liberty Reserve users were required to make any deposits or withdrawals through the use of third-party “exchangers.” In effect, this arrangement enabled the company to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail. The exchangers did not provide a reliable means of tracing financial activity, as they tended to be unlicensed money transmitting businesses operating in countries without significant governmental money laundering oversight or regulation, such as in Malaysia, Russia, Nigeria, and Vietnam. By failing to collect identifying information about its users through its website, and avoiding any contact with its users through the traditional banking system, Liberty Reserve intentionally provided its users with nearly impenetrable anonymity and enabled them to conduct untraceable financial transactions.

Liberty Reserve and several of its principals and employees were charged with conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business, and operation of an unlicensed money transmitting business.

Silk Road

Let me turn to the second case: Silk Road. As alleged, Silk Road was an underground website that emerged as the most sophisticated and extensive criminal marketplace on the Internet. Silk Road served as a sprawling black-market bazaar where unlawful goods and services -- primarily illegal drugs of almost every variety -- were bought and sold regularly by the site’s users. The volume of illegal transactions conducted on Silk Road was staggering. During its approximately two-and-a-half years in operation, Silk Road was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions. All told, the site generated sales revenue of more than 9.5 million Bitcoins and collected commissions from these sales totaling more than 600,000 Bitcoins.

Silk Road was designed to enable its users to buy and sell drugs and other illegal goods and services anonymously and beyond the reach of law enforcement. That was achieved in two principal ways. First, Silk Road was operated on the “TOR” network, a special network of computers on the Internet designed to conceal the true IP addresses, and therefore the identities, of the networks’ users. Second, the method of payment was deliberately restricted to preserve the users’ anonymity; transactions on Silk Road could be paid for only with Bitcoins, a decentralized virtual currency.

Silk Road’s payment system essentially consisted of an internal Bitcoin “bank,” where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address associated with the user’s Silk Road account. These addresses were stored on wallets maintained on servers controlled by Silk Road. In order to make a purchase on Silk Road, a user had to obtain Bitcoins (typically through a Bitcoin exchanger) and then send those Bitcoins to a Bitcoin address associated with his or her Silk Road account. Once a user’s account was funded in this way, the user was free to make purchases on Silk Road. Silk Road also used a so-called “tumbler” which, as the site explained,

“sen[t] all payments through a complex, semi-random series of dummy transactions...making it nearly impossible to link your payment with any coins leaving the site.” The “tumbler” was essentially an institutionalized and automatic form of money laundering.

Silk Road’s alleged creator and owner, Ross Ulbricht, was charged with narcotics conspiracy, conspiracy to commit computer hacking, and money laundering conspiracy.

Robert Faiella (“BTCKing”) and Charles Shrem

Let me turn to our third and most recent case. Just two days ago, our office brought forth charges in another Bitcoin matter. As alleged, Robert Faiella – using the name “BTCKing” – operated a Bitcoin exchange service directly on Silk Road that enabled Silk Road users to convert cash into Bitcoins anonymously. Faiella’s customers could then use those Bitcoins to make illegal purchases on Silk Road. Faiella never registered as a money transmitting business, and he conducted transactions in a manner designed to enable Silk Road users to maintain their anonymity.

To accomplish that, Faiella filled the orders for Bitcoins that he received from his Silk Road customers with the assistance of Charles Shrem, the CEO of a NYC-based Bitcoin exchange company. Shrem’s company was designed to enable customers to exchange cash for Bitcoins anonymously, that is, without providing any personal identifying information. For example, to fund the purchase of Bitcoins, customers were instructed to deposit, in person, specific amounts of cash into bank accounts controlled by a third-party cash processor. Customers did not have to provide any identifying information other than an email address. After obtaining Bitcoins for his customers with Shrem’s assistance, Faiella then sold the Bitcoins to Silk Road users at a markup.

Shrem’s company was registered as a money transmitting business and had certain anti-money laundering policies, which Shrem was responsible for enforcing as the company’s compliance officer. However, instead of enforcing those policies, Shrem deliberately advised Faiella how to circumvent them so that Faiella could continue doing business with the company, thereby generating significant revenue in transaction fees for Shrem’s company. Shrem was aware that Silk Road was a drug-trafficking website and that Faiella was running a Bitcoin exchange service on Silk Road, but he still helped Faiella conduct his operation. Shrem never filed a single Suspicious Activity Report despite the obvious red flags. In total, Faiella and Shrem converted more than \$1 million of cash into Bitcoins for Silk Road users – so that those users could make unlawful purchases on Silk Road.

Faiella and Shrem were each charged with conspiracy to commit money laundering and operating an unlicensed money transmitting business. Shrem was also charged with willful failure to file a suspicious activity report.

Government Concerns Regarding the Criminal Exploitation of Virtual Currencies

These cases illustrate a number of concerns with virtual currencies, including Bitcoins, as their use increases.

One concern is the combination of Bitcoin’s anonymity and its ease of movement. Both characteristics offer advantages but also can make it a magnet for criminality. The ease with which large amounts of Bitcoins can be moved anonymously (without any geographic limitation)

makes the currency particularly attractive to those conducting illegal activity. Although cash is also an anonymous form of currency, there are significant practical barriers to transferring bulk cash outside of the traditional banking system. Generally, to make such transfers, the bulk cash must be physically transported (or smuggled) from one place to another. By contrast, large amounts of Bitcoins can be transferred anonymously and safely to someone located anywhere in the world with just a click of a computer key.

A second concern is that virtual currency expands the geographic footprint of criminal activity and at the same time invites more criminal participants. For purchasers of drugs or other illegal goods or services, virtual currency reduces or even eliminates practical barriers to entry. On Silk Road, for example, users were able to purchase drugs from drug dealers located anywhere in the world, essentially with the push of a button. With traditional forms of currency, these purchasers would have had to hand-deliver cash to the drug dealers. Similarly, the anonymous and largely untraceable nature of Bitcoins also makes it attractive to sellers of unlawful goods. In addition to the thousands of drug dealers who operated on Silk Road, we found that the “merchants” who accepted Liberty Reserve currency were overwhelmingly criminal in nature.

Third, because the transactions not only are anonymous, but are irreversible, virtual currency also appeals to those operating fraudulent schemes. In frauds such as advanced fee schemes, the fraudsters often previously relied on traditional money transfer services to collect money from victims because they perceived those services as offering greater anonymity than the traditional banking system. Now, we have observed that these fraudsters are seeking to take advantage of virtual currency because of the even greater degree of anonymity it offers. The Liberty Reserve vendors, for example, included peddlers of various types of online Ponzi and fraudulent get-rich-quick schemes.

Fourth, virtual currency also facilitates the laundering of criminal proceeds, as it enables criminals to securely and anonymously distribute the proceeds of criminal activity to co-conspirators and others located anywhere in the world.

Fifth, the anonymous and untraceable nature of virtual currency also has tax implications, especially as the currency becomes more widely accepted. In terms of tax evasion, putting money into virtual currency may be a way to conceal it from the taxing authorities. The currency itself, then, could effectively become a form of tax haven for both businesses and individuals.

Sixth, as Bitcoins become more prevalent they will potentially create opportunities for investments based on their value. For example, people may invest in currency futures contracts tied to Bitcoins or in Bitcoin mining companies hoping for a return based on the amount of Bitcoins mined. Such an investment market based on a currency that is volatile and lightly regulated could lead to fraud based on manipulation and other analogs to securities fraud.

Conclusion

Virtual currencies, like Bitcoins, are innovative and dynamic new systems that may offer many benefits. These currencies present complex challenges to law enforcement in terms of identifying and locating criminals who corruptly exploit them. We have had some success, but it is difficult work in part because of the layers of anonymity and geographical distance that our investigations have to overcome. But for all those who not only believe in the rule of law but also hope for these

currencies to take root and thrive, they should support law enforcement's efforts to ensure that individuals who exploit virtual currencies for criminal purposes are held responsible. Whatever the regulators and others determine should be the role of virtual currencies, the prospects for these new currencies are severely damaged if they become the currencies of choice for criminals. We look forward to continuing our work with all our Federal, State and international partners to protect the people from criminal conduct, whatever the currency. Thank you for inviting me here today. I would be happy to answer any questions you may have.

USAO - New York, Southern

Updated May 13, 2015